

Description:

This course helps you prepare an organization to create a complete end to end solution for monitoring, preventing, detecting, and mitigating threats as they arise in real time.



Do not fool yourself, this course is far more advanced than you may expect. It is fast paced and thorough, so you can enjoy a well-rounded experience. Be ready to dig deep into the details of security analysis for today's needs.

You will be able to set up and deploy state of the art open source and commercial analysis tools, intrusion detection tools, syslog servers, and SIEMs. You will also be able to integrate them for an entire organization.

*This course maps to the mile2 Certified Cyber Security Analyst Exam as well as the Comp TIA CySA+CSO-001 certification exam.



Annual Salary Potential \$70,351 AVG/year

* CySA+ and CSO-001 are registered trademarks of CompTia

Key Course Information	Modules/Lessons	Labs
<p>Live Class Duration: 5 Days CEUs: 40 Language: English Class Formats Available:</p> <ul style="list-style-type: none"> Instructor Led Self-Study Live Virtual Training <p>Suggested Prerequisites: (Any of the following Mile2 Courses)</p> <ul style="list-style-type: none"> - Certified Security Principles - Certified Digital Forensics Examiner - Certified Incident Handling Engineer - Certified Professional Ethical Hacker - Certified Penetration Testing Engineer - or Equivalent Knowledge 	<p>Module 1 – Blue Team Principles</p> <p>Module 2 - Digital Forensics</p> <p>Module 3 – Malware Analysis</p> <p>Module 4 – Traffic Analysis</p> <p>Module 5 – Assessing the Current State of Defense within an Organization</p> <p>Module 6 – Leveraging SIEM for Advances Analytics</p> <p>Module 7 – Defeating the Red Team with Purple Team Tactics</p>	<p>Lab 1 – Establishing Ips and Logging into the VMs</p> <p>Lab 2 - Blue Team Principles</p> <p>Lab 3 – Digital Forensics</p> <p>Lab 4 – Malware Analysis</p> <p>Lab 5 – Traffic Analysis</p> <p>Lab 6 – Assessing Current State of Defense within an Organization</p> <p>Lab 7 – Leveraging SIEM for Advanced Analytics</p> <p>Lab 8 – Defeating the Red Team with Purple Team Tactics</p> <p>*All labs are performed in our Cyber Range® on our Ghost Pentesting Platform®</p>

Who Should Attend

- Security Professionals
- Incident Handling Professionals
- Anyone in a Security Operations Center
- Forensics Experts
- Cybersecurity Analysts

Upon Completion

Upon completion, the Certified Cybersecurity Analyst candidate will be able to competently take the C)CSA Exam. They will also be ready to prepare an organization for proactive defense against today's hackers.

Accreditations



Exam Information

The Certified Cybersecurity Analyst exam is taken online through Mile2's Learning Management System and is accessible on your Mile2.com account. The exam will take approximately 2 hours and consist of 100 multiple choice questions.

A minimum grade of 70% is required for certification.

Re-Certification Requirements

All Mile2 certifications will be awarded a 3-year expiration date.

There are two requirements to maintain Mile2 certification:

- 1) Pass the most current version of the exam for your respective existing certification
- 2) Earn and submit 20 CEUs per year in your Mile2 account.

Course FAQ's

Question: Do I have to purchase a course to buy a certification exam?

Answer: No

Question: Do all Mile2 courses map to a role-based career path?

Answer: Yes. You can find the career path and other courses associated with it at www.mile2.com.

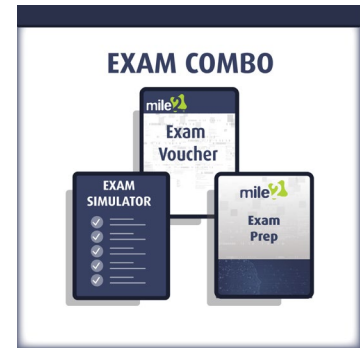
Question: Are all courses available as self-study courses?

Answer: Yes. There is however 1 exception. The Red Team vs Blue Team course is only available as a live class.

Question: Are Mile2 courses transferable/shareable?

Answer: No. The course materials, videos, and exams are not meant to be shared or transferred.

Course and Certification Learning Options



Detailed Outline:

Course Introduction

Chapter 1 - Blue Team Principles

- a. Network Architecture and how it lays the groundwork
 - i. Defensive Network
- b. Security Data Locations and how they tie together
- c. Security Operations Center
 - i. The People, Processes, and Technology
 - ii. Triage and Analysis
 - iii. Digital Forensics
 - iv. Incident Handling
 - v. Vulnerability Management
- d. Automation, Improvement, and Tuning

✱ Chapter 1 Labs – Blue Team Principles

- a. Analyze Initial Compromise Vector
- b. Network Forensics
- c. System Forensics

Chapter 2 - Digital Forensics

- a. Investigative Theory and Processes
 - i. Digital Acquisition
 - ii. Evidence Protocols
 - iii. Evidence Presentation
- b. Computer Forensics Laboratory
 - i. Protocols
 - ii. Processing Techniques
 - iii. Specialized Artifacts
- c. Advanced Forensics for Today's Exploitations

✱ Chapter 2 Labs – Digital Forensics

- a. Analysis of Captured Network Activity
- b. Analysis of Captured Zip File

Chapter 3 - Malware Analysis

- a. Creating the Safe Environment
- b. Static Analysis
- c. Dynamic Analysis
- d. Behavior Based Analysis
- e. What is different about Ransomware?
- f. Manual Code Reversing

✿ **Chapter 3 Labs – Malware Analysis**

- a. Analysis of an MSFVenom Executable
- b. Analysis of Locky Ransomware
- c. Creating YARA Rules based on Analysis Results
- d. Final Assessment

Chapter 4 - Traffic Analysis

- a. Manual Analysis Principles
- b. Automated Analysis Principles
 - i. Signatures compared to Behaviors
- c. Application Protocols Analysis Principles
- d. Networking Forensics

✿ **Chapter 4 Labs – Traffic Analysis**

- a. Traffic Analysis of a Website Defacement Attack
- b. Traffic Analysis Based on IDS Alerts
- c. Traffic Analysis of a ZLoader Delivery Attempt
- d. Bonus: Find the Backdoor!!!

Chapter 5 - Assessing the Current State of Defense with the Organization

- a. Network Architecture and Monitoring
- b. Endpoint Architecture and Monitoring
- c. Automation, Improvement, and continuous monitoring

✿ **Chapter 5 Labs – Assessing the Current State of Defense within the Organization**

- a. Configuring a Firewall
- b. Configuring SIEM
- c. Configuring IPDS
- d. Upgrading Detection/Protection Capabilities

Chapter 6 - Leveraging SIEM for Advanced Analytics

- a. Architectural Benefits
- b. Profiling and Baselining
- c. Advanced Analytics

✿ **Chapter 6 Labs – Leveraging SIEM for Advanced Analytics**

- a. Deploying Agent
- b. Implementing User Behavior Analytics through Machine Learning
- c. Simulate an Attack and Analyze Alerts

Chapter 7 - Defeating the Red Team with Purple Team tactics

- a. Penetration Testing with full knowledge
 - i. Reconnaissance
 - ii. Scanning
 - iii. Enumeration
 - iv. Exploitation
 - v. Lateral Movement

✿ **Chapter 7 Labs – Defeating the Red Team with Purple Team Tactics**

- a. Configuring Defensive Systems
- b. Purple Team Testing
- c. Mitigation
- d. Bypass Anti-Virus and LSASS Patch through edited Mimikatz